O. MANAGEMENT INFORMATION SYSTEM

In this section

This section contains the following topics:

O.1. Report Requirements

Policy: Required Reports

Listed below are all of the required reports as well as how often each report should be run. Please refer to the current WICNU Windows Application manual for a complete listing of reports available and details on running each report.

Report Name	Frequency
Beginning of Day	Automatically runs, clinic must print report
End of Day	Automatically runs, clinic must print report
Automated Termination	Automatically runs bi-weekly, monthly or bi-monthly. Interval is set by the clinic.
Purge Report	Automatically runs bi-weekly, monthly or bi-monthly. Interval is set by the clinic.
Potential Dual Application Report	Runs with BoD reports
Proration Override Report	Monthly
Unused voucher stock report	Weekly
Missed Appointment report	Weekly

Procedure

Many required reports require that research be done at the clinic level to resolve errors and findings on the report. Follow instructions to conduct research on reports and consult with the help desk as needed to correct any problems that cannot be corrected at clinic level.

I. All documentation must be done with pen. Be brief and to the point. Reference participant charts, names, other computer reports, check numbers or dates when necessary. Make sure your documentation can be understood by other individuals or auditors reviewing the documentation. You may use symbols or color coding as long as a key is provided explaining their meaning.

II. When using the computer system to document appropriate information:
   a. Be concise and to the point.
   b. Comments should be understandable to others

c. Do not delete comments.
d. If a priority comment is received during a transfer, contact the help desk if comments did not transfer to investigate what action may be necessary.

III. All reports must be securely bound and tagged or labeled by month and Federal Fiscal year.

a. One folder can contain one or more months of computer reports. A label should be placed on the front of each folder indicating which month(s) and year are included in the binder. Do not use rubber bands or paper clips to secure computer reports.

IV. Potential Dual Application Report

a. Refer to Section G.8 for detailed procedures

V. Proration Override Report

a. Document why the proration was overridden.
   i. Reasons must valid and comply with policy.
   ii. Reasons such as “participant needed the food” cannot be accepted.
   iii. Any inappropriate overrides must be documented in the comments as such and the staff involved must be counseled.
   iv. Refer to Section C.8 for further details

VI. Unused Voucher Stock Report

a. Gaps identified in the unused voucher stock report must be researched and resolved on a weekly basis.
b. Check stubs must be pulled to determine if the checks were issued or if they need to be voided.
c. Checks that were not issued should be voided on the computer.
d. If the check is found to have been issued contact the help desk to resolve the discrepancy.
e. Refer to Section E.9 for detailed instructions on resolving gaps in food instrument and cash value voucher sequence.

VII. Missed Appointment Report

a. Refer to Section G.3 for detailed instructions.

O.2. Computer System Security

Policy: Computer System Security and Training

Computer hardware and software must be protected from misuse.   Data integrity must be monitored and guarded against data theft, loss, and errors. Computer users must be trained on system use and security. Local agencies must coordinate with the State WIC Help Desk/DTS staff and county/local health department IT departments in providing for the security and training on the Management Information System (MIS) and computer hardware.

Procedure:

I. Local agencies should require each end user to sign an Acceptable Use Policy form. (This is commonly required by and coordinated with the County/Health Department IT Department)

II. At least every two years each local agency should conduct training on computer security which covers the following topics:

a. Computer access
b. Appropriate internet use
c. Protecting confidential participant information

III. User permissions must be maintained on file.

IV. Staff must be trained on the current WIC information system.

V. Staff should monitor the use of the computer system to prevent loss of data due to theft, errors, and misuse.

VI. Issues and errors with the computer information system and computer hardware should promptly be reported to the WIC Help Desk. The Error Report Form should be completed when program errors are discovered.

VII. Follow the policies and procedures described in the current computer system’s security plan.

VIII. Users must sign off/log off terminals when leaving the computer workstation. Each individual staff using the terminal must log in with their own security information; multiple users cannot utilize the same log in.

IX. Software unrelated to WIC, clinic operations or local health department business should not be loaded onto WIC owned machines.

X. Computer hardware should be kept in a secure environment during clinic hours; portable equipment not in use must be locked in a secure location to avoid theft.